Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2009 Proceedings

Americas Conference on Information Systems (AMCIS)

2009

Has Decreasing Innovation Hurt the Stock Price of Information Security Firms? A Time Series Analysis

Lara Khansa
Virginia Tech, larak@vt.edu

Divakaran Liginlal
University of South Alabama, dliginlal@gmail.com

Has Decreasing Innovation Hurt the Stock Price of Information Security Firms? A Time Series Analysis

Lara Khansa
Virginia Tech
larak@vt.edu

Divakaran Liginlal
University of South Alabama
dliginlal@gmail.com

ABSTRACT

Prior research has shown that information security breaches are beneficial to the stock price of information security firms, around the time that these security breaches are announced. We, however, show that the overall trend in the market value of information security firms has actually been stagnating, despite an increasing number of security threats that exploit vulnerabilities in information systems. We attribute this decrease in the stock price of information security firms, after controlling for overall market conditions, to insufficient innovation on the part of information security firms. We apply time series regression methods to analyze the relationship between R&D intensity and the stock price of information security firms. This empirical work provides a plausible explanation for the decrease in the stock price of information security firms, despite high demand for their products and services.

Keywords

Information security, innovation, stock price, time series regression.

INTRODUCTION

With the rapid growth of Internet-based commerce and business globalization, the IT infrastructures of firms have become increasingly vulnerable to a variety of malicious attacks. We compiled about 9,300 malicious attacks, discovered from 1998 to 2008, from the website of Symantec, a major vendor of antivirus software. The impact of these malicious attacks is assessed by subject matter experts as low, medium, or high. We represented these impact estimates on an interval scale from 1 to 3 and aggregated them yearly to obtain Figure 1.

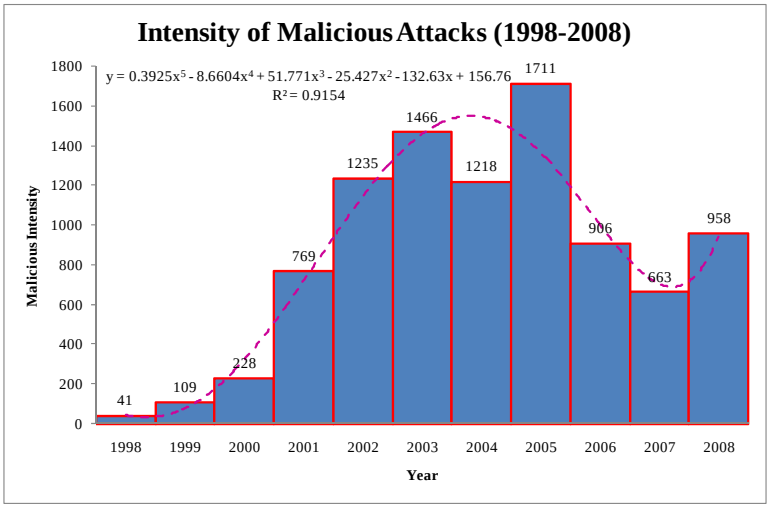

Figure 1. Frequency of Malicious Attacks

Figure 1 shows that the intensity of malicious attacks increased rapidly from 1998 to 2005, but has subsequently decreased. This is consistent with the results in Khansa and Liginlal (2007), who argued that regulatory compliance has been effective in motivating higher demand for enhanced security. Khansa and Liginlal (2009a) showed that investments in security safeguards helped decrease the severity of malicious attacks. Further, it has been shown in Khansa and Liginlal (2009b) that

when firms successfully incorporate information security within their business processes, they induce organizational learning and can flexibility switch amongst compatible information security technologies as the environment of malicious attacks varies.

Malicious attacks have been shown to impact the stock price of affected firms. Investors have frequently punished firms for the security and privacy breaches of their customers' information, whether these breaches are caused by outside malicious attackers or insiders. Ettredge and Richardson (2002) found that the stock price of both business to consumers (B2C) and business to business (B2B) firms dropped significantly during the test window around the February 2000 denial-of-service attacks. Kannan, Rees and Sridhar (2004) studied the change in market value of firms whose systems have been breached and showed that the announcement of a security breach decreases the market capitalization values of a firm. Liginlal, Sim and Khansa (2009) confirmed the negative effect on the market value of attacked firms of privacy breaches that occurred between 2005 to 2008. Campbell, Gordon, Loeb and Zhou (2003) found that only breaches related to confidential information have had a significant negative effect on the stock price of firms, while non-confidential breaches did not have any significant negative impact. Other authors like Telang and Wattal (2005) studied the impact of security breaches with exclusive attention to software vendors. They presented evidence that vulnerability announcements are adversely linked to the market prices of software vendors. While malicious attacks have been detrimental to the stock price of attacked firms, they were shown to have benefited information security firms, whose revenues are derived from developing safeguards against such attacks. Cavusoglu, Mishra and Raghunathan (2004) found that the market value of security firms increased by 1.36 percent during the two-day period following the announcement of an attack. Garg, Curtis and Halper (2003) confirmed this information transfer effect. Both of these studies have used event study analyses, but neither has attempted to investigate if this transfer effect is ephemeral or sustainable. In the remainder of this paper, we show that the information-transfer effect, reported in prior literature, is only momentary around the timing of security breaches and is not sustained.

Other than security breaches, innovation has been shown to affect the market value of firms and prior research has been ambivalent as to how the market values innovation. For example, Porter (1992) and Hall (1993) suggested that investors have a short time horizon and tend to undervalue rewards from long-term investments such as R&D. Jensen (1993), on the other hand, suggested that many firms' R&D investments are not profitable but investors systematically overlook this possibility, resulting in overvaluation of the stock. Doukas and Switzer (1992) showed that the market responds positively upon larger R&D spending, after accounting for differences in firms' knowledge capital bases. They also found a high rate of return to investment in R&D. Hall, Jaffe and Trajtenberg (2005) distinguished the impact of a firm's patents on its market value according to the time path and source of subsequent citations. They found that each ratio significantly affects market value, with an extra citation per patent boosting market value by 3%. They also showed that "unpredictable" citations have a stronger effect than predictable ones because market-value premiums are associated with future citations, rather than those received in the past. Finally, they showed that self-citations are, interestingly, more valuable than external citations. Ho, Keh and Ong (2005) also found that firms' spending on innovation, measured by R&D expenses, yields positive returns in terms of share price performance. Their findings, consistent with the resource-based literature, revealed that intensive investment in R&D contributes positively to the one-year stock market performances of manufacturing firms but not for non-manufacturing firms. Greenhalgh and Rogers (2006) found that the valuation of R&D varies substantially across sectors. In particular, they found that sectors that are the most competitive have the lowest market valuation of R&D. In addition, they showed that firms with larger market share have higher R&D valuations, supporting Schumpeter's theory (Shumpeter, 1934). Another example is Cho and Pucik (2005) who proposed the innovativeness–quality–performance model, which described how a firm's success in balancing innovativeness with quality drives growth and profitability, in turn driving superior market value. Particularly, in information systems, Subramani and Walden (2001) found that firms' e-commerce initiatives lead to significant positive cumulative abnormal returns to shareholders. In particular, they found that the cumulative abnormal returns for business-to-consumer (B2C) announcements are higher than those for business-to-business (B2B) announcements. Similarly, Kim, Cavusgil and Calantone (2006) linked innovation in information systems to the market value of the firm. They hypothesized that innovations, in the context of supply chain, can be viewed as firm resources that enhance channel capabilities and improve market performance.

Although information security complements information systems, the intricacies of information security innovation are governed by different dynamics. The main concern of information systems is the dissemination of knowledge in the fastest and most efficient means. Swanson (1994) proposed a typology of IS innovations that includes administrative and technical cores, in addition to a functional core that links the other two. While type I innovations are those that are confined to the functional IS task, type II innovations support the administration of the business and type III innovations are embedded in the core technology of the business. Implicit requirements in the design of an information system are performance, usability, and robustness according to known standards. When designing a system, the designer impersonates the user, with the inherent assumption of a benign environment where users have good intentions and threats are nonexistent. In contrast, information

security is inherently different in its assumptions of a hostile environment where threats are generated from inside and outside the system and malicious agents seek to cause failure. The goal of information security is, thus, to control the spreading of information by assigning circles of trust where only authorized users are allowed. While technology has facilitated the dissemination of information to achieve globalization through virtual boundaries, one may argue that information security technologies ensure 'freedom of silence'. Fisk (2002) noted that "the software industry is currently in a sub-optimal, but self-supporting equilibrium that does not support the effort required for software improvements". In other words, low level of demand for software has discouraged software firms from innovating. Different from the view of Fisk (2002), which has been shared with other researchers and industry experts, we show that the security firms' R&D intensity has been low, in spite of growing demand and we investigate the question: *Has insufficient innovation by information security firms been associated with a deterioration of their stock price?*

The rest of this paper is organized as follows. In Section 2, we present our conceptual model and hypothesis. We then discuss in Section 3 the research design, including data collection and measures. Section 4 discusses the results, i.e. time series analyses and regression. Finally, Section 5 summarizes the contributions and discusses the limitations of our work.

THEORY

Dissecting the Value of Information Security

Figure 2 helps to dissect the value of information security to the market as a whole. Khansa and Liginlal (2007) showed that regulatory compliance and malicious attacks necessitate that firms invest in information security to protect their IT infrastructures. Beside their direct impact on firms' investments in information security, malicious attacks positively moderate the effect of regulatory compliance on investment in information security. These two external stimuli, in turn, trigger market dynamics between consumers and producers of information security, and stock market investors. Demand for information security creates the need for more innovation, which, in turn, boosts investors' confidence in the information security sector. The beauty of this consumer, producer, and investor paradigm resides in its self-sustainability. Consumers of information security benefit from more competitiveness and business efficiency. Their spending on information security, in turn, generates more revenues and justifies more innovation on the part of information security producers, boosting their shareholders' value. Innovation is at the heart of this cycle interacting with demand, on one side, and the stock market on the other side.

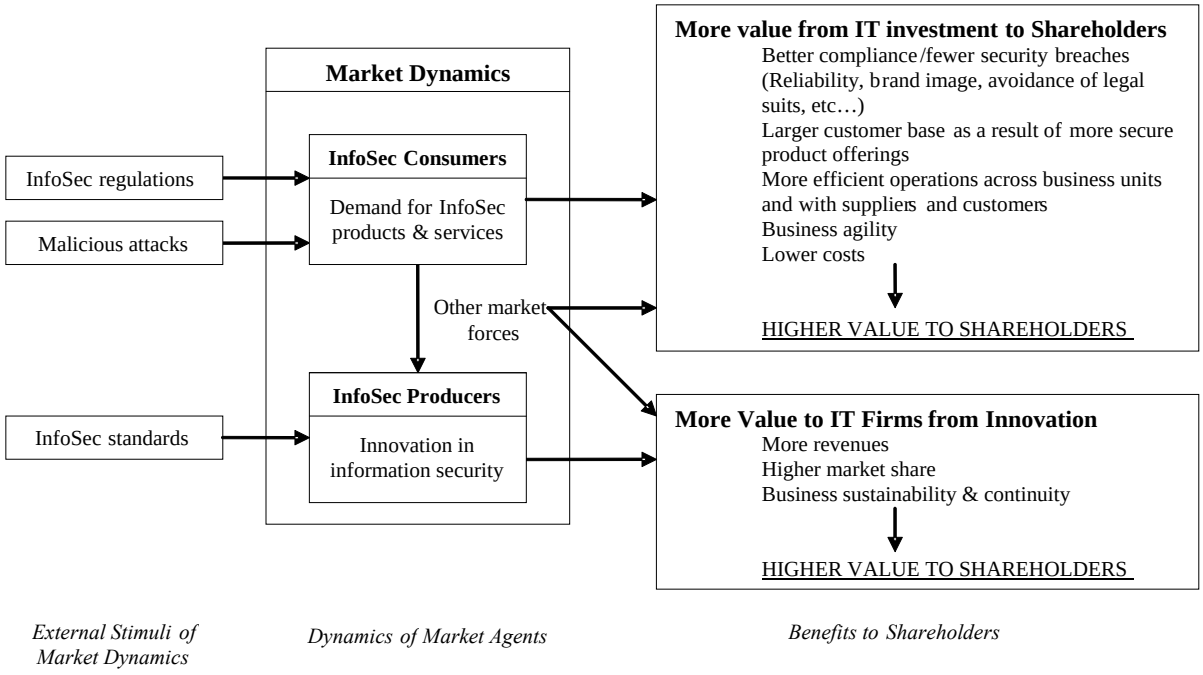

Figure 2. Where Does the Value of Information Security Lie? – A Conceptual Framework

Another aspect implicitly conveyed by the conceptual framework is the uniqueness of information security compared to other information systems. While the majority of information systems technologies were born out of a breakthrough innovation, information security is justified by the need to protect vulnerable IT systems. Furthermore, information security does not reside on a single layer of the IT architectural stack. Rather it plays multiple roles at all layers, making it an essential element of today's global economy.

Hypothesis

The market value equation (See Hall et al. (2005) for a detailed presentation of the material), suggests that the market value of a firm ought to reflect the value of all its assets, physical and intangible, i.e. its knowledge stock. Given that knowledge stock is the output of R&D investment, the market value equation implies that firms should invest in R&D to increase their shareholders' wealth. Equation 1 summarizes the market value equation assuming that the additively separable linear specification applies and that the marginal shadow value of assets are equalized across firms.

$$V_{it} = q_t(A_{it} + \gamma K_{it})^{\alpha} \quad (1)$$

V_{it} : *Market value of firm i at time t*

A_{it} : *Ordinary physical assets*

K_{it} : *Knowledge stock*

γ : *Shadow value of knowledge assets relative to tangibles*

α : *Allows for non − constant return to scale*

Prior literature (Erikson and Whited 2006) has similarly established that an increase in the innovation efforts of companies would result in better stock market performance because a firm should invest in assets, whether tangible or intangible, only if these assets are used by the firm towards creating at least as much market value as the cost of reproducing them; otherwise, the assets would be better employed elsewhere. Based on these results and on the market value equation, we attribute information security firms' losses in market value to the fact that their innovation has not kept up with increasing demand for their products and services. We, thus hypothesize the following:

> Hypothesis 1: *Insufficient innovation by information security firms has been associated with a deterioration of their stock price.*

RESEARCH DESIGN

Data Collection

We selected the various market segments of the information security sector, including antivirus, identity and access management, network security, and content security market segments. We then chose all public information security firms in the selected market segments. After screening off non-public firms and firms whose product offerings include other than information security products, only 33 representative firms remained, which encompass the following technology sectors and segments identified by unique SIC codes and sub-codes, (i) Security software and services (includes firms such as McAfee with stock ticker MFE), (ii) Internet software and services (includes firms such as Symantec (SYMC) and Verisign (VRSN)), (iii) Business software and services (includes firms such as Blue Coat Systems with stock ticker BCSI), and (iv) Computer peripherals (includes firms such as Secure Computing with stock ticker SCUR). By covering the period from the pre-Internet bubble (1998) to the end of 2008, this study is meant to be invariant to micro changes such as mergers and acquisitions or bankruptcies. Therefore, even if a firm gets acquired sometimes in this period, it is still included up until its acquisition. We chose the period from 1998 to 2008 because of its diversity in the sense that it includes the pre-bubble years, the years of the Internet bubble, the quasi recession of 2001, the subsequent short economic recovery, as well as the credit crisis of the late 2007and 2008. The inclusion of all these economic settings adds to the generalizability of our results.

Measure of Innovation

To quantify innovation, we first followed the lead of prior literature and conducted a patent count analysis. For that, we searched for patents in the database of the US Patents and Trademark Office under class 726, which corresponds to information security, and class 380, which relates to cryptography. Class 726 includes 36 subclasses listed at different

hierarchical levels encompassing data protection methods, antivirus techniques, and network-related security, while class 380 includes 122 subclasses, encompassing cryptanalysis, communication system cryptography, key management, and algorithmic function encoding among others. A thorough analysis of information security patents revealed that most information security patents filed before 1998 were cryptography-related as shown in Figure 3. The analysis indicates that patent count peaked in 2000 and dropped afterwards as shown in Figure 4.

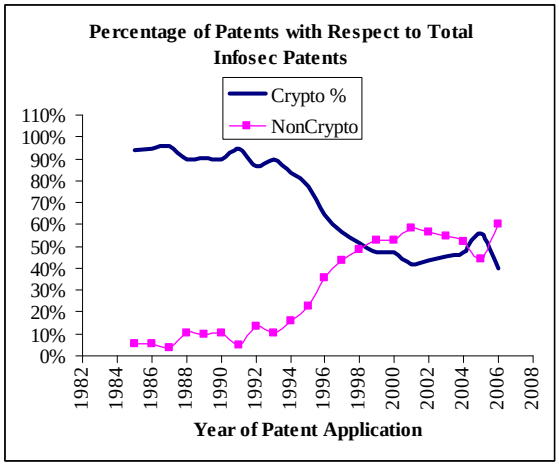

Figure 3. Annual Patent Percentage

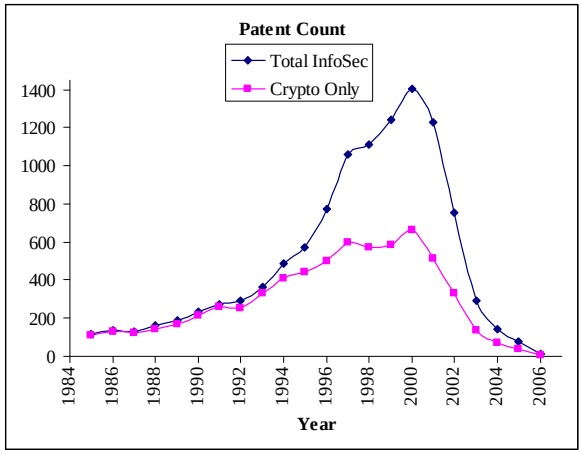

Figure 4. Annual Patent Count

The problem with patent count is that it is a very noisy indicator as it does not account for the value of patents: even if a firm files a large number of patents, the value of these patents is in no way guaranteed by their number. Another measure that has been used is patent citations (See Hall et al. (2005), for example), as the extent to which patents are cited is an indication for their worth. Information security, as an independent discipline, is pretty nascent and only thrived during the Internet bubble at the onset of the new millennium. Given that patents take, on average, five to six years to complete the review process, most patents filed after 2002 might still be under review. In fact, Figure 4 shows that the number of accepted patents that were filed after 2002 goes down sharply, further confirming that relying on patent-related measures is unreliable.

R&D expenses constitute another measure that does not suffer from data insufficiency. This measure has been widely used by researchers to quantify innovation in information security (See Ho et al. (2005), for example). The argument supporting the use of R&D expenses to measure innovation is that information security firms, like other technology firms, differentiate themselves by their knowledge stock rather than by their physical assets. Even though R&D is expensed, the outputs of these expenses have much higher tangible and intangible values. The tangible value resides in the new competitive products resulting from the R&D, while the intangible value carries brand name, customer base, trade secrets, and market competitiveness, among others. These R&D-generated assets are what make a technology firm. Using R&D expenses, as is, gives an absolute measure that is independent of demand. We use a related measure, namely R&D intensity, which is constructed as the ratio of R&D spending by the revenues of information security firms. This measure is better at capturing how intensive R&D activities are to meet demand. R&D intensity has been found to be a major determinant of firm market value and has been shown to be positively correlated with firm profits (Hirschey and Weygandt 1985; Cockbum and Griliches 1988; Megna and Mueller 1991). Table 1 summarizes the indices that we use in our subsequent time series analyses.

The Innovation Index	This index is a simple average of the R&D intensities of the firms in the selected sample. R&D intensity is the ratio of R&D expenses by sales.
The Market Value Index	This index is also a quarterly index, constructed as the average of the quarterly stock market prices of each firm in the sample.
The Market Return Index	This market return index controls for prevailing market conditions and was constructed from the quarterly levels of NASDAQ's value weighted returns.

Table 1. Indices

RESULTS

The plot of the NASDAQ-adjusted market value index (Figure 5) reveals that the market value of information security firms has been stagnating for the past six years. We constructed the data in Figure 5 by subtracting the effect of the NASDAQ index, which most of the information security firms in our sample belong to. Parallel to this slow growth in market value is a similar decrease in R&D intensity over the past six years, as shown in Figure 6.

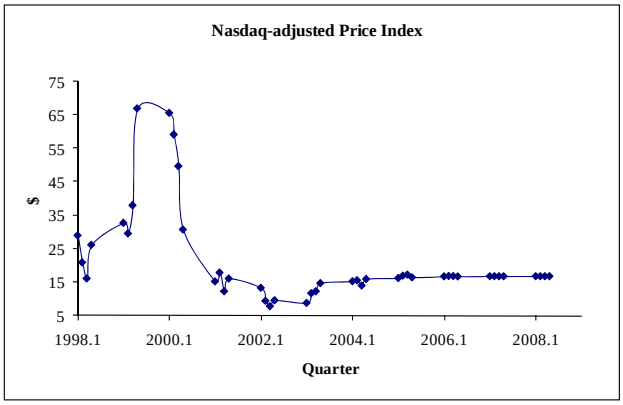

Figure 5. Market Value Time Series

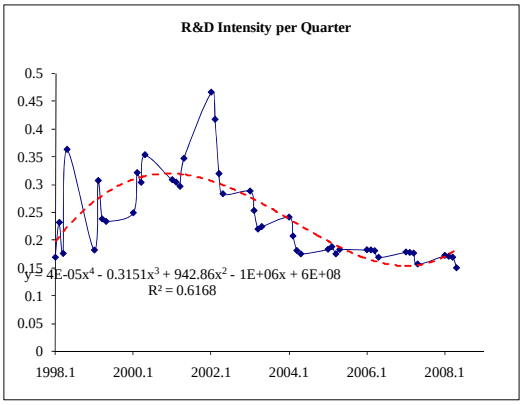

Figure 6. Innovation Time Series

In order to understand why R&D intensity has been decreasing, we looked at its components, namely R&D expenses and total sales. Recall that we have proposed sales (or revenues) of information security firms as a measure of demand. Revenues of information security firms, pictured in Figure 7, have been consistently rising at an approximate average rate of 0.24 MM$/Quarter ($R^2$ = 88.86 %). Figure 8 shows that R&D spending has been following a decreasing trend for the past six years. The slow growth rate of R&D spending and the highly increasing revenues of information security firms explain why R&D intensity has been decreasing and suggest that information security firms have not been spending on R&D at a rate that matches demand. Based on the market value equation, shown in Equation 1, we hypothesize that the decrease in R&D intensity of information security firms has been reflected negatively on their stock price.

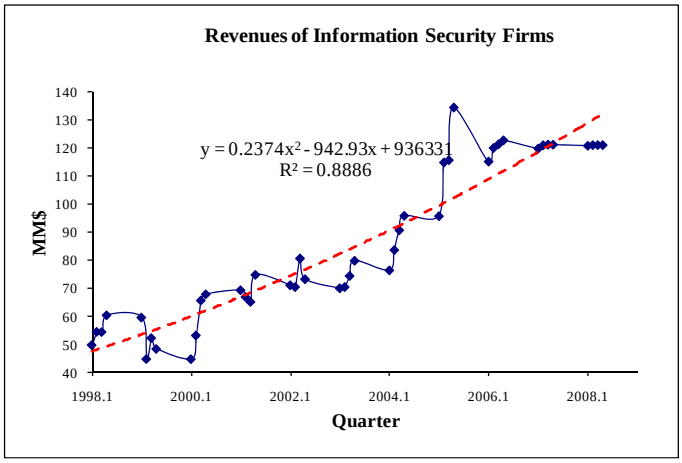

Figure 7. Revenues Time Series

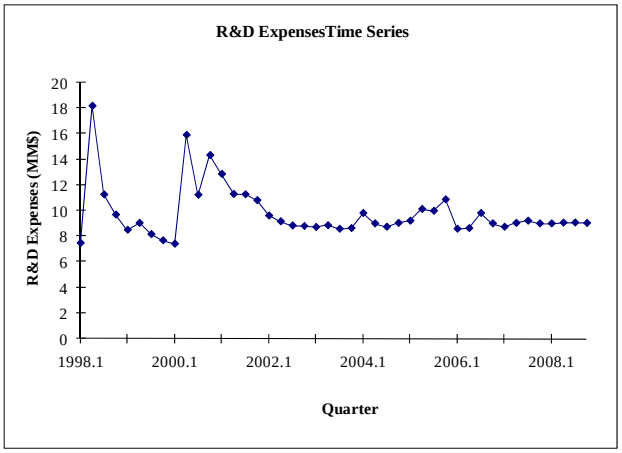

Figure 8. R&D Expenses Time Series

Time Series Regression

Before conducting time series regression analyses, all time series were analyzed for autocorrelation. The autocorrelation functions (PACFs) of the innovation index and the market value index revealed high first-order autocorrelations (0.8484 for the innovation index and 0.941 for the market value index). We performed lag-1 differencing on each of the two time series to remove their first-order autocorrelation. Using the indices in Table 1, we formulize Hypothesis 1 as follows:

$$StockPrice_t - StockPrice_{t-1} = a + b\left[NasdaqLevel_t + NasdaqLevel_{t-1}\right] + c\left[R\,\&\,D\ Intensity_{t-j} - R\,\&\,D\ Intensity_{t-j-1}\right] + \varepsilon_t$$

$$H_0:\ b > 0\ and\ \exists\ j : c > 0 \qquad (2)$$

The results in Table 2 show that, indeed, R&D intensity drives market value of information security firms at the 1% significance level (p-value < 0.01). That explains why the market value has been stagnating despite increasing demand for information security products and services. The Durbin-Watson test indicates the absence of autocorrelation (lower Durbin-Watson level=1.09 and upper Durbin-Watson level=1.35).

Independent Variables	***Coefficients***	***t Stat***	***P-value***
Lagged R&D Intensity; Lag=1 quarter	0.0105072	4.788	7.00E-05
Lagged Nasdaq Level	243.0203509	5.216	0.00E+00
Adjusted R-square	72.280%		
Durbin-Watson test	1.0898640		
Overall F test	40.11		

Table 2. Results of Time Series Regression

CONCLUSIONS, CONTRIBUTIONS, AND LIMITATIONS

Prior research, following the standard market value function, has shown that innovative activities, including R&D spending and patents significantly influence the market value of firms. In this study we have shown that the information-transfer effect on the market value of information security firms around the timing of security breach announcements is only temporary and not sustainable. The overall trend in the market value of information security firms has actually been stagnating despite growing trends in malicious attacks and vulnerabilities in information systems.

The major contribution of our work is the empirical evidence linking R&D intensity to the non-increasing market value of information security firms. Our conceptual framework, modeling the consumer, producer, and investor paradigm shows that the cycle of demand, innovation, and stock market investment can be self-sustained only if innovation, the key link is alive and thriving. Specifically, this work carries ample share of practical significance as it shows to executives of information security firms the necessity of innovating to generate shareholder wealth and ensure business continuity.

Given that our analysis is exploratory in nature rather than composing of a direct test, there are limitations to our study. There may be other factors that may be influencing the market value of security firms and their R&D expenditures. For example, if one takes an industry lifecycle view from the innovation literature, perhaps the industry is becoming more competitive over time and R&D spending naturally flattens out for these firms after they develop their initial products. Given that information security firms in our sample are medium-to-small, we argue, however, that their R&D spending should not yet have flattened.

Our ongoing research includes designing a questionnaire to interview CSOs of US firms to better gage what drives their demand for information security products and services. Understanding the drivers of demand will provide information security firms with a clearer picture of what to target when boosting their innovation efforts. Further, we intend to identify the factors that dampen information security firms' spending on R&D, giving insights to academic researchers as well as industry experts.

ACKNOWLEDGMENTS

We thank Dr. Elizabeth Regan, the mini-track Chair, and the anonymous reviewers for their valuable comments. Their suggestions were instrumental in improving the paper.

REFERENCES

1. Campbell K., Gordon L.A., Loeb M.P. and Zhou, L. (2003) The Economic cost of publicly announced information security breaches: Empirical evidence from the stock market, *Journal of Computer Security* 11, 3, 431-448.
2. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004) The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers, *International Journal of Electronic Commerce* 9, 1, 69-104.

3. Cho, H.J., and Pucik, V. (2005) Relationship between innovativeness, quality, growth, profitability, and market Value, *Strategic Management Journal* 26, 555-575.
4. Cockbum, I., and Griliches, Z. (1988) Industry effects and the appropriability measures in the stock markets valuation of R&D and patents, *American Economic Review* 78, 2, 419-423.
5. Doukas, J., and Switzer, L. (1992) The stock market's valuation of R&D spending and market concentration, *Journal of Economics and Business* 44, 2, 95–114.
6. Erickson, T. and Whited, T.M. (2006) On the accuracy of different measures of Q, *Financial Management* 35, 3
7. Ettredge, M. and Richardson, V. J. (2002) Assessing the risk in E-commerce, in *Proceedings of the 35th Hawaii International Conference on System Sciences*, 2673- 2682.
8. Fisk, M. (2002) Causes and remedies for social acceptance of network insecurity, *Workshop on Economics and Information Security*, University of California, Berkeley.
9. Garg, A., Curtis, J., and Halper, H. (2003) Quantifying the financial impact of IT security breaches, *Management & Computer Security* 11, 2, 74-83.
10. Greenhalgh, C. A., and Rogers, M. (2008) Intellectual property activity by service sector and manufacturing firms in the UK, 1996 – 2000, in H. Scarbrough (Ed.) The evolution of business knowledge, Oxford: Oxford University Press.
11. Hall, B.H. (1993) The stock market's valuation of R&D investment during the 1980's, *American Economic Review* 83, 259-264.
12. Hall, B.H., Jaffe, A., and Trajtenberg, M. (2005) Market value and patent citations, *Rand Journal of Economics* 36, 1, 16-38.
13. Hirschey, M.A, and Weygandt, J.J. (1985) Amortization policy for advertising and research and development expenditures, *Journal of Accounting Research* 23, l, 326-335.
14. Ho, K. Y., Keh, H.T., and Ong, J.M. (2005) The effects of R&D and advertising on firm value: An examination of manufacturing and nonmanufacturing firms, *IEEE Transactions on Engineering Management* 52, 1, 3-14.
15. Jensen, M.C. (1993) The modern industrial revolution, exit, and the failure of internal control systems, *Journal of Finance* 48, 831-880.
16. Kannan, K., Rees, J., and Sridhar, S. (2004) Reexamining the impact of information security breach announcements on firm performance, in *Proceedings of the Ninth INFORMS Conference on Information Systems and Technology (CIST)*.
17. Khansa, L. and Liginlal D. (2007) The Influence of regulations on innovation in information security, in *Proceedings of the 13th Americas Conference on Information Systems (AMCIS 2007)*, Keystone, CO, paper 180.
18. Khansa, L. and Liginlal D. (2009a) Quantifying the benefits of investing in information security, *Communications of the ACM*, forthcoming.
19. Khansa, L. and Liginlal D. (2009b) Valuing the flexibility of investing in security process innovations, *European Journal of Operational research* 192, 1, 216-235.
20. Kim, D., Cavusgil, S.T., and Calantone, R.J. (2006) Information system innovations and supply chain management: Channel relationships and firm performance, *Journal of the Academy of Marketing Science* 34, 1, 40-54.
21. Liginlal, D., Sim, I., and Khansa, L. (2009) How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management, *Computers and Security* 28, 3-4, 215-228.
22. Megna, P. and Mueller, D.C. (1991) Profit rates and intangible capital, *this REVIEW* 73, 4, 632-642.
23. Porter, M.E. (1992) Capital disadvantage: America's failing capital investment system, *Harvard Business Review* 70, 65-82.
24. Schumpeter, J.A. (1934) The Theory of Economic Development, Cambridge, Massachusetts: Harvard College.
25. Subramani, M. R., and Walden, E. A. (2001) The Impact of E-commerce announcements on the market value of firms, *Information System Research* 12, 2, 135-154.
26. Swanson, E. B. (1994) Information systems innovation among organizations, *Management Science* 40, 9, 1069–1088
27. Telang, R. and Wattal, S. (2005) Impact of vulnerability disclosure on market value of software vendors: An empirical analysis, *4th Workshop on Economics and Information Security*, Boston.